جامعة المستقبل
Mustaqbal University
أول جامعة أهلية بمنطقة القصيم

# Information Sharing Policies

Prepared by

**Information Technology Department &**

**Statistics and Information Department&**

**Media and Institutional Communications Department**

**January 2025**

# Contents

Chapter 1

# Authorized Entities to Store and Share University Information

## 1.1 Types of Information and Publication Policy

University information is divided into main categories based on its degree of publicity and confidentiality, and can be presented simply as follows:

Public Information: This is information that the university makes available to the public without restrictions, and is often published on the official website or in informational guides.

Examples:

- The university's vision, mission, values, and strategic objectives.

- Published regulations, bylaws, and policies, such as open data policies, council manuals, and the organizational structure.

- Study programs, general admission requirements, the academic calendar, and university news and events.

Internal Non-Confidential Information: This is information that is not for public release but is available to university affiliates (faculty members, staff, and sometimes students) through internal portals.

Examples:

- Minutes of some academic and administrative councils that are not published to the public. - Internal performance reports, detailed departmental plans, and operational work procedures.

- Certain administrative and organizational databases that do not directly affect the privacy of individuals.

Confidential Information: This is information whose disclosure could harm individuals or the university and is protected by data protection regulations and electronic systems.

Examples:

- Personal data of students, faculty, and staff (academic records, ID numbers, financial data, health records).

- System login credentials and any data that affects information security, cybersecurity, or the internal/financial security of the university.

Highly Confidential Information: This is a highly sensitive subcategory within "confidential" and is often restricted by very limited access.

Examples:

- Eergency, security, and safety plans whose disclosure could compromise security.

- Certain major financial contracts, internal investigations, audit reports, or legal cases before their resolution.

- Any information that the university designates in its policies as "restricted" or "highly confidential." Important Organizational Notes

- The university links these categories to its privacy, cybersecurity, and open data policies, specifying what may be published, what must be protected, and how to handle it.

- Refer to the Information Security Policy in the university's "Information Technology Management" manual and the Privacy Policy on the portal to learn how to protect personal and confidential information.

## 1.2 Information Storage Entities

Many entities within the university are authorized to store information in both hard copy and electronically. The most important of these are:

- The Office of the University President

- Secretariat Offices

- The Documents and Records Department

- Electronic Archiving Systems

- The Quality and Accreditation Department

- The Statistics and Information Unit

## 1.3 Internal and External Information Exchange Entities

Many entities are authorized to exchange information internally, including:

- The Office of the University Rector

- Secretariat Offices

- The University's Electronic Platform

- The Quality and Accreditation Department

- The Statistics and Information Unit

- The Media and Institutional Communications Department

The university designates specific entities and individuals authorized to exchange information externally, after verifying its permissibility for publication. These include:

- The Office of the University Rector
- The Media and Institutional Communications Department
- Liaison officers authorized by senior management.

## Chapter 2

# Policies Related to the Electronic Portal

## 2.1 Electronic Portal Concepts

• The portal is the official website of Mustaqbal University and all related content publishing sites, whether they are college, department, faculty member, staff, or student websites.

• Terms of Use are all the terms and conditions that must be observed when using the Mustaqbal University portal.

• Content includes texts, graphics, advertisements, links, and other materials such as university news, events, videos, contact information for university staff, course materials, and published articles.

• External Links are links that redirect browsing to pages not affiliated with the Mustaqbal University portal.

## 2.2 Terms of Use

• The portal is the only official website of Mustaqbal University and is managed by the Information Technology Department, specifically the Software and Portal Management Section. Content is managed by the university's colleges, departments, and centers, each according to its own role.

• The university makes the portal's Terms of Use available on all pages of the portal.

• Users must understand that their use of the Mustaqbal University portal constitutes acceptance of the portal's Terms of Use. If they do not accept these terms in their entirety, accessing this site or any sub-site constitutes a violation, and they must cease using it immediately.

## 2.3 Subdomain Registration

• Mustaqbal University's websites are hosted on the World Wide Web by the university itself, other government entities, or hosting providers licensed by the Communications and Information Technology Commission. Hosting must be within the Kingdom of Saudi Arabia, and the contract between the parties must include safeguards to ensure data confidentiality.

• Each entity within the university is entitled to register a domain name or shortcode to be affiliated with the university's domain (uom.edu.sa) by submitting an official letter to the Information Technology Department specifying the desired shortcode.

• No entity within Mustaqbal University is permitted to create a website outside the (uom.edu.sa) domain.

## 2.4 Content Input and Update Authority

• The responsibility for adding, deleting, or modifying tabs on the university portal's homepage rests with the Software and Portal Department of the Information Technology Department at Mustaqbal University, or its designee.

• The responsibility for managing the university's online newspaper lies with the university's Media and Corporate Communications Department, which has full authority to publish and update the newspaper's content, including all news, events, seminars, conferences, articles, and related services.

• Any entity within Mustaqbal University wishing to publish news, events, seminars, articles, or conferences on the university's main portal must officially contact the university's Media and Communications Center.

• If a software addition is required (such as an attendance registration form, for example), the Software and Portal Section of the Information Technology Department must be provided with an official letter, submitted through administrative communication channels, outlining the request at least three weeks before the conference or event date. Failure to do so will result in the request being disregarded.

• Each university entity has its own independent website with full management authority. The dean or director of each entity is responsible for publishing and updating its online content. Each faculty member, staff member, and student also has their own independent website. • The Information Technology Department is not obligated to review external links connected to the portal, and the department bears no responsibility for the content or services offered by websites registered outside the official university portal.

## 2.5 Publishing on the Portal

• The portal is an electronic publishing platform for all university staff and departments. They are required to use it in a manner that benefits the university, its staff, and its various departments, and in a way that does not in any way harm the reputation of the university or its staff or expose them to legal liability.

• All content published on the portal pages must comply with copyright laws. Therefore, the following are prohibited, but not limited to:

- Any electronic materials not owned by the page owner and subject to copyright.

- Research papers published in scientific conferences and journals.

- Books and publications available in any electronic format.

- Inappropriate content, including but not limited to:

o Content containing offensive, abusive, racist, or threatening language, whether in text, image, or idea.

o Content that violates state and university regulations or societal norms.

o Content that infringes upon the privacy of others in any way.

• Every university department with a website on the university portal must ensure that all page content and materials are up-to-date, including news, contact information, phone numbers, email addresses, material descriptions, and other relevant information.

• Everyone must use the correct grammar and spelling rules for creating any webpage or electronic material and ensure its accuracy and freedom from errors.

• The Information Technology Department reserves the right to modify or delete information on any university-affiliated website at any time without prior notice if the portal's publishing and content management policies are violated.

### Privacy

• The Information Technology Department at Mustaqbal University is required to make the privacy policy available on all pages of the portal, clarifying the rights and obligations of the university website, its affiliated sites, and its users. Mustaqbal University is committed to protecting the confidentiality and privacy of its users.

• Privacy policies outline how Mustaqbal University handles users' personal information, whether it is stored online or on computers.

• Some links on the Mustaqbal University website connect to other websites not affiliated with the university (not within the domain (uom.edu.sa)). These websites do not operate in accordance with the Mustaqbal University website's privacy policy. Therefore, visitors should review the privacy policies of those websites before disclosing any personal information that could identify them.

## 2.6 Supervision and Training

• Each department within the university has the right to assign one or more supervisors. These supervisors are granted the necessary permissions for their university account used in the login system and are responsible for the department's website, its content, and all tasks necessary to ensure the website's continued operation.

• The Information Technology Department is committed to providing the necessary training for website management (for any department with a website under the portal umbrella). This training can be coordinated or requested through an official letter to the Information Technology Department.

• Every faculty member and those of equivalent status at the university has the right to receive the necessary training for managing their personal page within the faculty members' pages.

• Faculty members and those of equivalent status have the right to receive the necessary training for managing their personal pages within the faculty members' pages or departmental websites, in direct coordination with the Information Technology Department.

## 2.7 Internal Network Policies

• The use of a connection is not permitted. VPN access is permitted only when necessary and for specific individuals as follows:

o Individuals authorized to provide emergency technical support for any of the university's electronic systems.

o System administrators designated by the service owner.

o Suppliers approved by the IT department after the necessary supplies and installations have been completed.

• The service is requested according to a pre-defined workflow approved by the Dean of the IT department.

• The IT department is responsible for encrypting the authorized personal accounts used to connect to the university network via the SSL VPN service while traversing unsecured and untrusted networks.

• Password complexity requirements must be met in accordance with the user password management policy.

• Authorized university personnel must ensure that unauthorized users are not allowed to share the university's VPN services, obtain their passwords, or access and use the computer during the connection process.

• All computers connected to the university network via the VPN service are secured according to the IT department's antivirus software standards, using the latest versions of their files and the latest operating system security patches.

• Only approved computer applications may be used to establish connection channels. Using the University Network via VPN

• Authorized employees will automatically lose access to the university network via VPN after one hour of inactivity.

• Access to the computer of authorized employees using VPN will be restricted according to their work needs.

• The IT department is responsible for inspecting, monitoring, and reviewing all VPN connections at Mustaqbal University.

• Granting a VPN connection to users outside of Saudi Arabia is prohibited except in cases of necessity. The IT department reserves the right to approve or deny such requests.

• The IT department reserves the right to monitor, restrict, or disconnect any VPN connection for any purpose without prior notice.